In the Claims

1-6. (Canceled)

7. (Currently Amended) A method for enabling graphic-based linking to the internet, comprising:

receiving digital data corresponding to an initial graphic image, the data representing pixels, each having a value;

receiving plural bit address information;

processing the initial graphic image in accordance with the plural bit address information, thereby subtly changing the values of said represented pixels to yield an encoded graphic image having the address information steganographically encoded therein; and

distributing **a version of** the encoded graphic image data to users, who can decode the address information therefrom and use same in establishing a link to the internet.

8. (Previously Presented) The method of claim 7 in which the encoded graphic image conveys said plural-bit address information notwithstanding transformation into or out of digital form.

9. (Previously Presented) The method of claim 7 in which the address information is not recognizable as such to human viewers of a rendered version of the encoded graphic image.

10. (Original) The method of claim 7 in which the address information comprises a URL.

11. (Original) The method of claim 7 in which the address information comprises an index to a remote data structure, the remote data structure having a corresponding URL address stored therein.

12. (Previously Presented) The method of claim 7 in which the encoded graphic image conveys said address information notwithstanding transformation into or out of digital form.

13. (Previously Presented) The method of claim 7 in which the initial graphic image comprises a photographic image.

14. (Previously Presented) A computer readable storage medium having stored thereon an encoded graphic image encoded according to claim 7.

15. (Previously Presented) The method of claim 7 in which the initial graphic image is a color image, rather than a grayscale image.

16. (Previously Presented) A method for enabling graphic-based linking to the internet, comprising:

receiving digital data corresponding to a graphic image;

steganographically encoding the graphic image to hide plural bit address information therein; and

distributing the encoded graphic image data to users, who can decode the address information therefrom and use same in establishing a link to the internet;

wherein the steganographic encoding is adapted in strength in accordance with local characteristics of the graphic image, said adaptation comprising more than two different strengths.

17. (Previously Presented) A method for enabling graphic-based linking to the internet, comprising:

receiving digital data corresponding to a graphic image;

steganographically encoding the graphic image to hide plural bit address information therein; and

distributing the encoded graphic image data to users, who can decode the address information therefrom and use same in establishing a link to the internet;

wherein said distributing comprises distributing the encoded graphic image data in digital, rather than hardcopy, form.

18. (Previously Presented) A method for enabling graphic-based linking to the internet, comprising:

receiving digital data corresponding to a graphic image;

steganographically encoding the graphic image to hide plural bit address information therein; and

distributing the encoded graphic image data to users, who can decode the address information therefrom and use same in establishing a link to the internet;

wherein the plural-bit address information is encoded redundantly through the graphic image, wherein all of said plural bits can be recovered both from first and second non-overlapping excerpts of said image.

19. (Previously Presented) A method of initiating access to a computer via a data communications medium, the method comprising:

receiving artwork corresponding to an object to be printed, the artwork including text and background;

steganographically embedding into at least the background of said artwork certain information indicative of an address associated with said computer; and

printing said object using the artwork into which said information has been steganographically embedded.

20. (Previously Presented) A physical object printed on a substrate and including text and background, at least the background being of continuous tone and having a plural-bit code steganographically embedded therein, said code being an index to a data structure that specifies address information of a computer resource that is to be associated with said object.

21. (Previously Presented) The object of claim 20 wherein said data structure is maintained on a computer separate from the computer whose address information is to be associated with the object.

22. (Previously Presented) A method for graphic-based linking to a computer address, comprising:

receiving digital data at a user's computer, the data corresponding to a graphic image;

using plural-bit index data steganographically decoded from said graphic image digital data to index a database;

obtaining from said database a URL address corresponding to said plural-bit index data;

establishing a link to said URL address; and

presenting a screen display on the user's computer in accordance with information obtained from said URL address.

23. (Previously Presented) A method of initiating access to a computer via a data communications medium, the method comprising:

providing first data indicative of an address associated with the computer;

steganographically embedding the first data in a second object comprising visual data, said embedding occurring in-band within said visual data, rather than in a part of said second object not intended for presentation to a user;

decoding from the second object the steganographically embedded first data; and

initiating a link to the computer using the first data.

24. (Previously Presented) The method of claim 23 wherein the first data comprises a URL address.

25. (Previously Presented) The method of claim 23 wherein the first data comprises an index number for use in accessing a data base.

26. (Previously Presented) The method of claim 23 that includes performing said decoding and initiating in the same device.

27. (Previously Presented) The method of claim 23 in which the second object is in digital form, and is not rendered into human-perceptible form between said embedding and decoding.

28. (Previously Presented) The method of claim 23 that includes distributing the second object to at least certain members of the public between said embedding and decoding.

29. (Previously Presented) A method of initiating access to a computer via a data communications medium, the method comprising:

providing first data indicative of an address associated with the computer;

steganographically embedding the first data in a second object comprising visual data, said embedding extending generally throughout a sampled representation of said second object, rather than localized in a particular portion thereof, wherein the complete first data can be recovered from an excerpt of said second object and used to initiate a link to the computer.

30. (Previously Presented) The method of claim 29 in which the second object is represented by plural samples, and said embedding changes a majority of said samples.

31. (Previously Presented) The method of claim 29 in which the second object is represented by plural samples, and the embedding is relatively weaker in regions where it might more readily be perceived.

32. (New) A method comprising:

at a first device, receiving data representing a graphic, the graphic having non-uniformly toned regions with information steganographically encoded therein;

decoding the steganographically encoded information from the received data;

communicating with a second, remote device;

receiving data from the remote device; and

controlling an aspect of operation of the first device in accordance with said data received from the remote device;

wherein the data received from the remote device is a function of information decoded from the received data.

33. (New) The method of claim 32 wherein said steganographic encoding is adapted in strength in accordance with features of the graphic data, said adaptation comprising more than two different strengths.

34. (New) The method of claim 32 wherein said steganographic encoding is manifested as extra pseudo-random noise in the received graphic data.

35. (New) The method of claim 32 wherein said controlling includes presenting a web page on the first device, the contents of said web page depending on data received from the remote device.

36. (New) The method of claim 32 that includes using said decoded information to identify a node on a computer network, said node comprising the remote device.

37. (New) The method of claim 32 wherein the remote device comprises a server computer.

38. (New) The method of claim 32 that includes controlling output presented to a user of the first device in accordance with the data received from the remote device.

39. (New) The method of claim 32 wherein the remote device is identified in accordance with the information decoded from the received data.

40. (New) The method of claim 32 that includes producing the received graphic data from a non-digital representation thereof.

41. (New) The method of claim 40 that includes producing the received graphic data by scanning a tangible medium with visible light

42. (New) A method comprising:

at a first device, receiving data representing audio, said data having information steganographically encoded therein;

decoding the steganographically encoded information from the received data;

communicating with a second, remote device;

receiving data from the remote device; and

controlling an aspect of operation of the first device in accordance with said data received from the remote device;

wherein the data received from the remote device is a function of information decoded from the received data.

43. (New) The method of claim 42 wherein said steganographic encoding is adapted in strength in accordance with features of the audio data, said adaptation comprising more than two different strengths.

44. (New) The method of claim 42 wherein said steganographic encoding is manifested as extra pseudo-random noise in the received audio data.

45. (New) The method of claim 42 wherein said controlling includes presenting a web page on the first device, the contents of said web page depending on data received from the remote device.

46. (New) The method of claim 42 that includes using said decoded information to identify a node on a computer network, said node comprising the remote device.

47. (New) The method of claim 42 wherein the remote device comprises a server computer.

48. (New) The method of claim 42 that includes controlling output presented to a user of the first device in accordance with the data received from the remote device.

49. (New) The method of claim 42 wherein the remote device is identified in accordance with the information decoded from the received data.

50. (New) The method of claim 42 that includes producing the received data from a non-digital representation thereof.

51. (New) A method comprising:

receiving audio data; and

steganographically encoding machine readable data in the audio data, the machine readable data identifying a computer implemented process that is to be invoked when the steganographic encoding is decoded and acted upon by a computer device.

52. (New) The method of claim 51 wherein said steganographic encoding is adapted in strength in accordance with features of the audio data, said adaptation comprising more than two different strengths.

53. (New) The method of claim 51 wherein said steganographic encoding is manifested as extra pseudo-random noise in the received audio data.

54. (New) The method of claim 51 wherein said computer implemented process includes communicating with a remote computer, and controlling information presented to a user in accordance with data received from said remote computer.

55. (New) A method comprising:

receiving graphic data; and

steganographically encoding machine readable data in the graphic data, the machine readable data identifying a computer implemented process that is to be invoked when the steganographic encoding is decoded and acted upon by a computer device.

56. (New) The method of claim 55 wherein said steganographic encoding is adapted in strength in accordance with local characteristics of the graphic data, said adaptation comprising more than two different strengths.

57. (New) The method of claim 55 wherein said steganographic encoding is manifested as extra pseudo-random noise in the received graphic data.

58. (New) The method of claim 55 wherein said computer implemented process includes communicating with a remote computer, and controlling information presented to a user in accordance with data received from said remote computer.

59. (New) A tangible medium comprising an encoded graphic, the graphic comprising non-uniformly toned regions that are steganographically encoded to convey machine readable data, wherein said machine-readable data serves to elicit a processing action corresponding thereto when decoded by a first computer device

60. (New) The tangible medium of claim 59 wherein said encoding is adapted in strength in accordance with local characteristics of the graphic, said adaptation comprising more than two different strengths.

61. (New) The tangible medium of claim 59 wherein said steganographic encoding is manifested as extra pseudo-random noise in the encoded graphic.

62. (New) The tangible medium of claim 59 in which said data serves to trigger linking of said first computer device to a second computer device, the second computer device being determined in accordance with said data.

63. (New) The tangible medium of claim 59 in which the processing action includes communicating with a second computer device, receiving data from said second device, and controlling an aspect of operation of the first device in accordance with said received data.

64. (New) A method comprising:

receiving an index number;

by reference to said index number, obtaining from a database an identification of a node on a computer network corresponding thereto;

establishing a link to said identified node;

receiving information from said node; and

controlling operation of a user device in accordance with information received from said node;

wherein the index number is based on information decoded from a steganographically encoded creative data object.

65. (New) The method of claim 64 wherein said creative data object represents a graphic having regions of non-uniform tone, and said index number is steganographically encoded in said regions.

66. (New) The method of claim 64 wherein said creative data object represents audio.

67. (New) The method of claim 64 in which said controlling includes directing a web browser on the user device to present information received from said identified node.

68. (New) The method of claim 64 wherein a web browser performs said decoding of the steganographically encoded creative data object.

69. (New) A network-connected device characterized by a decoder that decodes information steganographically encoded within a creative data object, the device utilizing

said decoded information to elicit an action by a remote computer, said remote computer transferring information to said device through the network in accordance with information decoded from the creative data object.

70. (New) The device of claim 69 wherein the creative data object represents audio.

71. (New) The device of claim 69 wherein the creative data object represents a graphic having non-uniformly toned regions with said information steganographically encoded therein.

72. (New) The device of claim 69 in which said decoded information comprises address information, and the device includes a web browser that loads a web page identified by said address information

73. (New) The device of claim 69 wherein said steganographic encoding of said data object is adapted in strength in accordance with features of the object, said adaptation comprising more than two different strengths.

74. (New) The device of claim 69 wherein said steganographic encoding is manifested as extra pseudo-random noise in the data object.